Hellenic Public Administration Certification Authority (APED)

Time Stamping Authority Disclosure Statement

Version 1.0

Version History

Date	Version	Changes
15/12/2021	1.0	Αρχικό έγγραφο

1. Overview

This document aims to provide the Subscriber and Relying Parties of a Qualified Time Stamp with a quick recap concerning the information available in APED's TSA Certificate Policy and Certificate Practice Statement and APED's Terms and Conditions for Use Qualified Trust Services.

This document does not substitute or replace APED's Terms and Conditions for Use of Qualified Trust Services nor the Certificate Policy and Certification Practice Statement; it summarizes the key points for the benefit of Subscribers and Relying Parties.

2. Contact Info

Hellenic Public Administration Certification Authority (APED)

Qualified Trust Service Provider

Address:
Ministry of Digital Governance
Directorate of e-Governance
11 Fragoudi str. & Al. Pantou, GR-101 63 Kallithea

e-mail: aped@mindigital.gr
Phone: 210-9098505

3. Electronic Time-stamp Types and Usage

Policy applied

The APED Time Stamping Authority Certificate Policy & Certification Practice Statement is based on the ETSI BTSP best practices policy for time-stamps (OID 0.4.0.2023.1.1)

Types of Time Stamps, Expected Lifetime of Time Stamp

Time stamps issued by APED are qualified under the eIDAS Regulation. The qcStatement "esi4-qtstStatement-1" as defined in ETSI EN 319 422 is used as an indication that the timestamp is a qualified electronic time-stamp.

Time Stamping Services can be used either independently or in combination with a Qualified Certificate for Electronic Signature or Seal, in order to prove that data in electronic form existed at a particular time.

The expected validity period of APED TSU is five (5) years.

Cryptographic hash functions, used in the timestamping process are in accordance with normative requirements, SHA-256 and SHA-512.

Time-stamp usage

The Time Stamping Services shall not be used outside of the limits and contexts specified in APED's Time Stamping CP & CPS and for unlawful purposes, or contrary to public interest. Indicatively, the use of Time Stamps is prohibited for any of the following purposes:

- unlawful activity (including cyber-attacks);
- issuance of new Time Stamps and information regarding Time Stamp validity;
- enabling other parties to use the Subscriber's Time Stamp Service;
- using the Time Stamp issued to time-stamp documents which can bring about unwanted consequences (including time-stamping such documents for testing purposes).

Information about verification of the time-stamp

Time Stamps can be verified as described in Section 5 and 6 of the present document.

4. Reliance Limits

Validity of Time Stamps

Time Stamps become valid as of the date specified in them. The validity of the Time Stamp expires on the date of expiry indicated in the Time Stamp or if the TSU Certificate is revoked.

APED TSA ensures that the Time Stamp Unit's private signing keys are not used beyond the end of their life cycle.

The Time Stamp Token generation system shall reject any attempt to issue a Time Stamp Token if the signing private key is expired or if the signing private key usage period is expired.

Accuracy of time

APED ensures that Time Stamp Tokens are issued securely and include the correct time. The APED TSA ensures that its time is synchronised with UTC within the declared accuracy with multiple independent time sources. The TSTs are issued with an accuracy of one (1) second. APED implements security controls preventing unauthorised operation, aimed at calibration of TSA time. APED monitors that synchronization is maintained when a leap second occurs.

Maintenance of event logs

APED ensures that

- all TSA control and event logs concerning the Time Stamping Unit (TSU) certificate are retained for at least seven (7) years after the expiration of the TSU certificate
- all TSA control and event logs concerning Time-Stamping services are retained for at least one (1) year after the expiration of the TSU Certificate

Time Stamping Unit certificates are valid for five (5) years but require re-keying every year.

5. Obligations of Subscriber

Subscribers shall verify the signatures created by the APED TSA on the TST.

Such verification comprises:

- Verification whether the TSA signature on the TST is valid.
- Verification of the TSA certificate.

Subscribers must use secure cryptographic functions for time-stamping requests. Subscriber obligations are also defined in APED's Terms and Conditions for Use of Qualified Trust Services.

6. TSU Public Key Certificate Status Checking Obligation of Relying Parties

Relying parties shall verify the signatures created by the APED TSA on the TST. Such verification comprises:

- Verification whether the TSA signature on the TST is valid.
- Verification of the TSA certificate.

Relying Parties should take into account any limitations on usage of the time stamp indicated by the APED Time Stamping Authority Certificate Policy & Certification Practice Statement. If the verification takes place after the end of the validity period of the Certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421.

Relying parties are expected to use a Trusted List to establish whether the time-stamp unit and the timestamp are qualified.

7. Limited Warranty Disclaimer / Limitation of Liability

For warranty and liability limitations, please refer to the Terms and Conditions for Use of Qualified Trust Services published on APED's website at https://pki.aped.gov.gr/repository

8. Applicable Agreements, CP, CPS

Relevant agreements, policies and practice statements are:

- APED Certificate Policy and Certification Practice Statement for Qualified Time Stamping Services
- APED Terms and Conditions for Use of Qualified Trust Services.

Current versions of all applicable documents are publicly available in the APED repository https://pki.aped.gov.gr/repository

9. Privacy Policy

APED processes personal data in accordance to the applicable data protection legislation in force. For further details, please refer to APED Privacy Statement at https://pki.aped.gov.gr/repository

10. Repository Licenses, Trust Marks and Audit

APED's Trusted Services for Qualified Electronic Signatures and Qualified Time Stamps are registered at Hellenic Telecommunication & Post Commission (E.E.T.T.) Trusted List of Qualified Trust Service Providers:

https://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/EsignProviders.html

and at the relevant EU Trusted List:

https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

The prerequisite requirement of this registration is in compliance with applicable regulations and standards. The Conformity Assessment Body is accredited in accordance with Regulation (EC) No 765/2008 as competent to carry out conformity assessment of the Qualified Trust Service Provider and qualified Trust Services it provides. Audit conclusions or certificates, which are based on audit results of the conformity assessment conducted pursuant to the eIDAS Regulation, corresponding legislation and standards are published on APED's website https://pki.aped.gov.gr/repository

11. Applicable Law, Complaints, Dispute Resolution

Any disputes related to the Trust Services provided by APED shall be governed by the laws of Greece. The Subscriber must notify APED of the dispute, any claim or complaint not later than thirty (30) calendar days after the detection of the basis of the claim, unless otherwise provided by law.

If the dispute is not resolved within sixty (60) days after the initial notice, then a party may seek legal resolution. Courts of Athens, Greece, shall have exclusive jurisdiction and venue for hearing and resolving any dispute.